

Exploring information technology, the Internet, biotechnology and life science issues

Many companies ill-equipped to handle hackers

■ Corporate security begins on the technical side, say experts from Dominant Systems

Security is related in many people's minds to metal detectors and locks on doors. And though many companies think they have computer security under control, most experts in the business disagree.

Computers are an integral part of almost all businesses, and a large amount of information, often confidential and crucial information, is stored on a company server or network.

Though screen passwords and security cameras can help the problem, they simply aren't enough, according to Terrence Weadock, founder and President of **Dominant Systems**, a network security firm in Ann Arbor.

Weadock and his associates pointed out the top network security concerns and problems in corporate America.

"We're so dependent on networks, but so many companies don't take the initiative to protect them," he said. "If the wrong person gets in, they can really foul up your corporation."

Firewalls are critical to every company that has an Internet connection, Weadock said. They control what is going into and coming out of the Internet while connected, and therefore prevent improper parties from viewing the information.

"A lot of companies aren't aware of the risk of having missing or improperly installed firewalls," Weadock said. "They don't realize they're just leaving their front door wide open."

While often companies take some security measures in the office, the home gets overlooked, Weadock said. Many companies allow their employees remote access to the company server or network, but if the proper firewalls are not installed there as well, it's like leaving a back door wide open, according to Network Consultant Laura Packard.

Another common mistake companies make in regards to computer security is allowing everyone access to everything, Weadock said. Though it's easier to just let all of a company's employees have the same account that can access anything - accounting files, technical information, even public

relations - it can be dangerous, Weadock said. If a disgruntled employee or former employee can get into one account that has access to all company information, much more damage can be done as opposed to limited and selected file access.

"You need to look at who is allowed to do what, and why," Weadock said. "Letting employees do anything they want is a bad move. You have to go through your employees person by person and figure out what they need to do their job, and give them that. This can really protect a lot of information if people hack into it."

A surprise to many companies is that old software is easier to hack into, Weadock said.

"Any network operating system has holes," he explained. "As the holes are discovered, the manufacturers will fix it and release a patch, upgrade or service pack. Many times security holes are discovered after it is installed. You have to be fairly religious about patches being installed, especially on servers. Just because it's working doesn't mean it's not broken."

"None of this is automatic," Packard said. "You have to fix the server yourself. If you never touch the software after you put it in, you're almost guaranteed to be at risk."

"A server is like a car: it requires maintenance," said Jeff Nanney, Manager of Tech Services.

Along those same lines, when the software is installed, it should never be left in the default configuration set up by the manufacturer, as it contains lax security measures, Weadock said. It is better to hire someone to install it or have someone on staff that can set it up with proper security settings.

A more basic security measure of simply monitoring who is using the network and when is important as well, Weadock said. It should be set up as corporate policy, and he said most companies don't do this. He said keeping track of when employees use the computer room or who has access to certain things should be written out and expressed to employees.

"It's a common sense thing most companies don't have a policy for," he said.

Excessive file and directory access controls, such as NFS exports and NT shares pose a problem because it allows anyone to attach to anything on the



Photo by Jennifer Beasley

From left, Terrence Weadock, founder and President of Dominant Systems, Jeff Nanney, Manager of Technical Services, and Laura Packard, Network Consultant, specialize in network security and disaster recovery.

network, and if one computer is broken into, he or she has access to everything, Weadock said.

And passwords, one of the most common security measures, often defeat their own purpose because they are weak, easy to figure out, and reused. Words that can be found in the dictionary can be hacked into instantly, Weadock said, and even alpha characters combined with numeric aren't always enough. He said it should be a combination of alpha, numeric and symbols such as a dollar sign or exclamation point to make it the most difficult and cumbersome to figure out, even with password searching programs, which are easily accessible. He also suggested a 7- or 14-character password, as many Microsoft programs break a password up into two passwords of seven characters, or seven and whatever is leftover. Weadock said a nine-character password can be easy to figure out with the right software, as the last two characters can be found quickly, and then the other seven can be broken into separately.

Lastly, logging and monitoring services are important for a company's security. Weadock said many companies wouldn't even know if they're hacked into without these services, as copying files and stealing information won't leave an obvious footprint. With these services, companies can track

who is in the network and what they're doing or using, and fix the problem if a hole is found.

One of the services Dominant Systems offers is an Internet security scan. The company will actually attempt to break into a company's network and show them where the holes are and how to fix them. Weadock said one of the best ways to know if you're secure is to actually see how easy or difficult it is for an average hacker to break in.

"We're not master hackers, but we could probably break into most of the networks in this county," he said. Weadock recommends a book called *Hacking Exposed*, which tells the secrets of breaking into programs and how to do it yourself. He said it is a good reference to have so companies know how and where people get in.

By Jennifer Beasley, IBJ

Reprinted With Permission From
IBJ
The Insider Business Journal